Although particular embodiments (methods, systems, and configured media) of the present invention are expressly illustrated and described herein, it will be appreciated that other embodiments may be formed according to the present invention. Also, unless otherwise expressly indicted, the description herein of an embodiment of the present invention in one category (e.g., a method) extends to corresponding embodiments in the other categories (e.g., a system).

As used herein, terms such as "a" and "the" and item designations such as "application" are generally inclusive of one or more of the indicated item. In particular, in the claims a reference to an item generally means at least one such item is required.

The invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. Headings are for convenience only. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by patent is:

Sub a1

1. A method of providing transport-independent secure communications in a computer network, comprising the steps of:

receiving application data at an upper connection layer, the application data received from an application;

passing the application data from the upper connection layer to a security layer;

encrypting the application data within the security layer;

passing the encrypted application data from the security layer to a lower connection layer; and

sending the encrypted application data from the lower connection layer out a network connection;

wherein the application is not required to perform security handshakes in order to send encrypted application data over the network, the connection layers support at least one network transport protocol, and the security layer is not specific to that transport protocol.

2. The method of claim 1, further comprising the steps of receiving at the lower connection layer encrypted application data which came in at the network connection; passing the encrypted application data from the lower connection layer to the security layer; decrypting the application data within the security layer; passing the decrypted application data from the security layer to the upper connection layer; and sending the decrypted application data from the upper connection layer to the application, without requiring that the application perform a security handshake.

3. The method of claim 1, further comprising the step of the lower connection layer establishing a connection with a handshake mode that is at least one of an interactive mode and a blind-root-accept mode.

4. The method of claim 1, further comprising the step of the lower connection layer establishing a connection with a handshake mode that is at least one of a server mode, a client mode, and a server with client authentication enabled mode.

5. The method of claim 1, further comprising the step of changing a list of trusted roots for the secure connection.

6. The method of claim 1, further comprising the step of the security layer informing at least one of the connection layers of security handshake proceedings.

7. A system for secure computer networking, comprising:

an application which is free of code for performing security procedure handshakes for secure network communications;

at least one connection layer interfaced with the application, the connection layer comprising an upper connection layer and a lower connection layer, the connection layers comprising code for performing at least one network transport protocol; and

a security layer callable from the connection layer rather than the application, the security layer comprising code for performing security procedure handshakes for secure

network communications, the security layer also comprising code for encrypting and decrypting application data.

8. The system of claim 7, wherein the connection layers comprise code for performing a WinSock network transport protocol.

9. The system of claim 7, wherein the security layer comprises code for performing security procedure handshakes for a Secure Sockets Layer session.

10. The system of claim 7, wherein the security layer comprises code for performing security procedure handshakes for a Transport Layer Security session.

11. The system of claim 7, wherein the application comprises code for providing Lightweight Directory Access Protocol services.

12. The system of claim 7, comprising a means for the security layer and at least one of the connection layers to identify a particular application and its cryptographic properties.

13. The system of claim 7, comprising a means for the security layer and at least one of the connection layers to identify a function as a call back function.

14. The system of claim 7, comprising a means for establishing a secure connection using a specified handshake mode.

15. The system of claim 7, further comprising a legacy application which performs security handshakes, and a security module supporting a secure connection to the legacy application.

16. A configured storage medium embodying data and instructions readable by a computer to perform a method of processing application data for secure network communications, the method comprising the computer-implemented steps of:

at a security layer, receiving a request from a lower connection layer to establish a secure connection;

in response, utilizing a means for establishing a connection to establish the requested connection; and

at the security layer, receiving encrypted application data from the lower connection layer, decrypting the application data, and passing the decrypted application data to an upper connection layer;

whereby an application receives the decrypted application data without being required to perform security procedure handshakes for secure network communications.

17. The configured storage medium of claim 16, wherein the means for establishing a connection establishes a Secure Sockets Layer connection.

18. The configured storage medium of claim 16, wherein the method further comprises receiving the encrypted application data at the lower connection layer using a transport model.

19. The configured storage medium of claim 18, wherein the lower connection layer uses a Novell proxy transport model.

20. The configured storage medium of claim 16, further comprising a signal embodied in the computer, the signal comprising a secure network communications protocol stack interface which is callable from at least the lower connection layer.